PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 3 : H04L 9/02, H04K 1/04 H04J 3/04	A1	(11) International Publication Number: WO 85/ 00259
		(43) International Publication Date: 17 January 1985 (17.01.85)

(21) International Application Number: PCT/US84/01022

(22) International Filing Date: 29 June 1984 (29.06.84)

(31) Priority Application Number: 509, 111

(32) Priority Date: 29 June 1983 (29.06.83)

(33) Priority Country: US

(71) Applicant: M/A-COM DCC, INC. [US/US]; 11717 Exploration Lane, Germantown, MD 20874 (US).

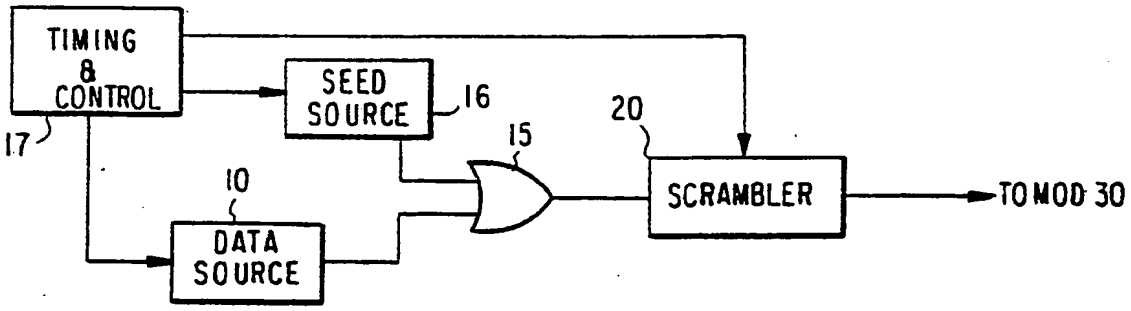
(72) Inventors: CORRIGAN, John ; 2209 Belmont Road, N.W., #403, Washington, C.D. 20009 (US). ROOS, David, A. ; 17312 Amity Drive, Gaithersburg, MD 20877 (US). TYAN, Shu-gwei ; 17552 Wheat Fall Drive, Derwood, MD 20855 (US).

(74) Agent: GREEN, Stanley, B.; Pollock, Vande Sande & Priddy, 1990 M Street, N.W., Washington, DC 20036 (US).

(81) Designated States: DE, DE (European patent), FR (European patent), GB, GB (European patent), JP.

Published
With international search report.

(54) Title: PROBABILISTIC SCRAMBLER AND METHOD OF PROBABILISTIC SCRAMBLING



(57) Abstract

Probabilistic scrambling, and the complementary probabilistic descrambling, for purposes of assuring reasonably frequent transitions in a transmitted signal for the purposes of receiver clocking. The transmitter (30) is provided with apparatus (16) for generating one or more different seeds. For transmitting any particular message, a seed is selected. The seed is generated randomly in order to increase the probability of successful transmission. The seed is used to generate a scrambling bit sequence which is combined with the data for transmission to generate a transmitted signal. The transmitted signal include at least some information identifying the scrambling bit sequence or the particular seed used for generating the scrambling bit sequence. Preferably, the seed itself (in scrambled or unscrambled form) precedes the scrambled data. At the receiver, (40) this seed is used to generate a complementary descrambling bit sequence which is combined with the received data to generate the original data scrambled at the transmitter (30).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**KR**	Republic of Corea
AU	Australia	**LI**	Liechtenstein
BE	Belgium	**LK**	Sri Lanka
BG	Bulgaria	**LU**	Luxembourg
BR	Brazil	**MC**	Monaco
CF	Central African Republic	**MG**	Madagascar
CG	Congo	**MR**	Mauritania
CH	Switzerland	**MW**	Malawi
CM	Cameroon	**NL**	Netherlands
DE	Germany, Federal Republic of	**NO**	Norway
DK	Denmark	**RO**	Romania
FI	Finland	**SD**	Sudan
FR	France	**SE**	Sweden
GA	Gabon	**SN**	Senegal
GB	United Kingdom	**SU**	Soviet Union
HU	Hungary	**TD**	Chad
JP	Japan	**TG**	Togo
KP	Democratic People's Republic of Korea	**US**	United States of America

PROBABILISTIC SCRAMBLER AND METHOD OF PROBABILISTIC SCRAMBLING

DESCRIPTION

Technical Field

The present invention relates to signal conditioning for communication purposes, and more particularly to conditioning a digital signal for the purposes of communication.

Background Art

The present invention relates to improvements in scramblers and improved methods of scrambling. The prior art has employed the term "scrambling" to denote processes used for two different purposes, although both processes are employed in the communication field.

The term scrambling has been used to describe the signal conditioning which is performed to render it difficult or impossible for unauthorized individuals to "eavesdrop" or intercept communications. The scrambling combines the data to be transmitted (typically in digital form) with a secret key (also in digital form) or some derivative of that secret key. Although unauthorized third parties may be capable of intercepting or eavesdropping on the result of the scrambling operation, in the absence of knowledge of the key, it is impossible, or at least difficult for the unauthorized individuals to extract the original data from the result of the combination. By pre-arrangement, authorized individuals have access to the key, and using the key can retrieve the original data from the combination which had been transmitted. This operational process is also sometimes referred to as enciphering or encryption, see for example Patent 4,221,931.

However, the prior art also employs the term "scrambling" to refer to an operation performed for an entirely different purpose. Digital data, which one desires to transmit, is, from the point of view of the communication equipment, entirely random. It is not at all unusual for the receiver equipment in a communication system to rely on data transitions in the received message to synchronize a receiver clock. Because of the random nature of the data that is being transmitted, however, there is no assurance that the data will exhibit transitions at a sufficiently rapid rate to maintain the receiver clock in synchronization with the transmitter clock.

In addition, some communication media exhibit non-uniform transfer functions as a function of frequency. Furthermore, it is not unusual for the transfer function of the communication media to vary not only with respect to frequency but with respect to time as well. To combat this non-uniformity, the signal being communicated should exhibit frequency components which are relatively widely distributed throughout the available bandwidth. Again, however, because the data to be transmitted is entirely random, there is no assurance that the frequency components of the data to be transmitted will be relatively widely distributed throughout the available bandwidth.

To overcome these, and similar problems, the prior art employs a scrambling process wherein the actual data to be transmitted is combined with another bit sequence (on a bit by bit basis using for example an exclusive OR operation) to produce a signal for transmission purposes. The parallel bit sequence (or scrambling bit sequence) is chosen so that the resulting signal to be transmitted has a higher probability of exhibiting transitions than would relatively random data. Viewed in another light, the scrambling sequence is employed to increase the probability that the energy in the transmitted signal is widely distributed

throughout the available bandwidth, than would be true in respect of the raw data to be transmitted.

The former described scrambling can be referred to as "encryption scrambling" and the latter as "dispersal scrambling" (merely for convenience). The invention deals with improvements in dispersal scrambling, hereinafter referred to as scrambling.

The key to successful use of such a scrambling operation depends, of course, on the fact that the receiver has information from which it can describe the scrambling bit sequence so that a complementary process carried out at the receiver with the received signal and the scrambling bit sequence can be employed to recover the data as it existed prior to its being combined with the scrambling bit sequence at the transmitter.

In the prior art, much effort has been made to select scrambling bit sequences which exhibit the desirable properties of regularizing the transitions in the transmitted signals and/or distributing the frequency components of the transmitted signal throughout the available bandwidth. Typically, in the prior art data scrambler, the transmitter and receiver use, on a repetitive basis, the same bit scrambling sequence. In other words, the transmitter and receiver use the same bit scrambling sequence over and over to transmit different messages. In this regard see for example U.S. Patent 4,214,209.

While the foregoing methods and apparatus work quite well for their intended purpose, they do exhibit varying degrees of effectiveness. The transmitted signal, resulting from the combination of a fixed bit scrambling sequence with a varying or random data to be transmitted, results in a transmitted signal. The scrambling function is selected to increase the percent of time that the transmitted signal

exhibits those desirable properties described above. However, since the scrambling sequence is fixed, it cannot guarantee that the transmitted signal resulting from any data sequence will still exhibit these desirable qualities. In fact, for any scrambling bit sequence, there are data sequences which result in a transmitted signal which does not have, or does not have to the desired degree, these desirable qualities. Depending on the particular communications system, some of the transmitted signals will not be correctly received. In this connection, the term data is that information, communication of which is the desired end result. A scrambling (or descrambling) bit sequence is a bit sequence which, when combined with the data to be transmitted, produces the transmitted signal or when combined with the received signal produces the data which is being communicated.

There is quite a common procedure in the communication field which is employed to determine when a received signal has been correctly received. Furthermore, it is also quite common in the event that a received signal is determined to have been inaccurately received, to request a retransmission thereof. To the extent that the communication system exhibits time varying parameters, the retransmission may result in a received signal which is correctly received on the second or third retry, etc.

However, insofar as the scrambling function is being effected, prior art communication systems do not exhibit time varying parameters, i.e. on the second and subsequent retries, the system will attempt to transmit the identical data which had been incorrectly received on the first try by scrambling that data with the same fixed scrambling bit sequence. Of course, the result will be identical in the second and third retries. Accordingly, to the extent that the scrambling bit sequence is selected which produces a transmitted signal having less than desirable properties on

a particular data sequence, the scrambling techniques will not improve the probability that the transmitted signal will be received correctly nor will the probability of correct receipt vary on the second or subsequent retries.

This prior art scrambling method and apparatus can be characterized as deterministic. More particularly, the scrambling bit sequence is fixed, the data to be transmitted (on second or subsequent retries) does not change and as a result the transmitted signal (the combination of the foregoing signals) is also identical. If the transmitted signal exhibits undesirable properties the first time it is created, it will exhibit the identical properties each time it is created.

It is therefore one object of the present invention to improve the effectiveness of scrambling by eliminating the deterministic nature of scrambling.

The foregoing feature of the invention can be implemented at the transmitter, by arranging the transmitter to produce scrambling bit sequences which may be different at different times, or for different messages, etc. Complementary changes are necessary at the receiver for the following reason. In the prior art, inasmuch as the scrambling bit sequence was fixed, the receiver employed the identical bit sequence in its descrambling operation. By making the changes at the transmitter noted above, it is no longer possible to employ a fixed bit sequence for the descrambling operation. More particularly, the bit sequence used in the descrambling operation must be identical to the bit scrambling sequence used in the scrambling operation. To this end, therefore, the receiver must be provided with some arrangement from which the bit sequence for use in the descrambling operation can be predicted or determined.

One technique for providing the receiver with knowledge of the bit sequence used in the scrambling operation is to transmit, at the same time as, prior to, or immediately subsequent to, the time the message is transmitted, the bit scrambling sequence as well. Alternatively, the message can be accompanied with (either preceded by, followed by or transmitted in parallel to) some data which is sufficient to define the bit scrambling sequence. This data can be a seed from which the entire bit scrambling sequence can be derived, or it can be a sequence number which either directly identifies the scrambling bit sequence or which directly identifies a seed from which the bit scrambling sequence can be derived. Other alternatives will be apparent to those skilled in the art.

Accordingly, to the extent that the bit scrambling sequence used at the transmitter (and the corresponding bit scrambling sequence used for the descrambling operation) varies from time to time, or message to message, the present invention provides a probabilistic scrambling apparatus and a method for probabilistic scrambling. The adjective probabilistic indicates the fact that one cannot determine from a given data sequence, the nature of the signal that will be transmitted (the combination of the data sequence and the bit scrambling sequence). The transmitted signal resulting from this combination cannot be determined because the bit sequence used for the scrambling operation is not fixed, but instead varies.

Accordingly, in one aspect the invention provides a method of scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking comprising the steps of:

a. generating a scrambling bit sequence;

b. combining said scrambling bit sequence with said data for transmission to generate a transmitted signal, wherein the improvement comprises:

c. periodically generating different scrambling bit sequences for combination with said data.

In accordance with a further specific feature of this aspect of the invention, the step (a) can comprise:

i. generating a seed,

ii. loading said seed into a shift register,

iii. shifting said seed through said register to generate said scrambling bit sequence,

wherein said step (c) includes periodically generating a new seed.

In another aspect, the invention provides a method of scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking comprising the steps of:

a. generating a scrambling bit sequence,

b. combining said scrambling bit sequence with data for transmission to generate a transmitted signal,

wherein the improvement comprises:

c. including bits in said transmitted signal identifying said scrambling bit sequence.

In accordance with a more specific feature of this aspect, the invention provides a method wherein said bits

identifying said scrambling bit sequence comprise a seed for generating said scrambling bit sequence.

A still further aspect of the invention provides apparatus for scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking, comprising:

means for generating a scrambling bit sequence,

means for combining said scrambling bit sequence and data for transmission to generate a transmitted signal, wherein the improvement comprises:

apparatus for controlling said means for generating a scrambling bit sequence for periodically generating different scrambling bit sequences.

A still further, more specific aspect of the invention is provided wherein said means for generating a scrambling bit sequence comprises:

means for generating a seed,

means for loading said seed into a shift register,

and means for shifting said seed through said shift register to generate said scrambling bit sequence, wherein said means for controlling said means for generating a scrambling bit sequence includes means for periodically generating a new seed.

Brief Description of the Drawings

The present invention will now be described in further detail so as to enable those skilled in the art to make and use the same in the following portions of this specification

when taken in conjunction with the attached drawings in which like reference characters identify identical apparatus and in which:

Figure 1 illustrates a typical communication link employing a scrambling and descrambling method and apparatus;

Figure 2 schematically illustrates the scrambling and/or descrambling function;

Figure 3 is a block diagram of the apparatus associated with a conventional scrambler in accordance with the method and apparatus of the invention;

Figure 4 is an example of a suitable scrambler for use in accordance with the method and apparatus of the invention;

Figure 5 is a block diagram of the descrambler and the apparatus associated therewith in accordance with the method and apparatus of the present invention; and

Figure 6 is a detailed schematic of a suitable descrambler for use in accordance with the method and apparatus of the invention.

Detailed Description of Preferred Embodiments

As shown in Figure 1, an apparatus for communicating digital information from a data source 10 to a data sink 60 includes a scrambling device 20 responsive to signals provided by the data source 10 and providing an output to a modulator 30. The output from the modulator 30 (a transmitted signal) may be transmitted to a remote location at which a demodulator 40 responds to the received signal and provides an output to a descrambler 50. The output of the descrambler 50 is provided to the data sink 60. Those skilled in the art will understand that Figure 1 only shows those portions of the

communication link which are relevant to the scrambling and descrambling operation, i.e. other conventional apparatus has not been illustrated.

Figure 2 is a schematic illustration of a typical scrambling or descrambling process. Figure 2 illustrates a gate 5, with inputs at A and B, and an output at C. The gate 5 may, for example, be an XOR gate. To the two inputs are applied the data to be transmitted (B) and a scrambling bit sequence (A). The result at output C is the signal for transmission, i.e. the scrambled data.

The same apparatus can be used to perform a descrambling operation. In this case, a bit sequence is applied at input A (in this case we can refer to it as a descrambling bit sequence), and to the input B the transmitted (or received) signal, i.e. scrambled data is applied. The result, at output C is the original data.

In the prior art scrambling or descrambling processes, the bit sequence (input A) was fixed, i.e. it repeated periodically. In accordance with the invention, on the other hand, Figure 3 shows apparatus associated with the scrambler 20 in order to effect probabilistic scrambling.

As shown in Figure 3, the data source, instead of being directly connected to an input of the scrambler 20, is coupled to the scrambler 20 through a gate 15. A timing and control apparatus 17 is added for purposes of controlling transmission of data from data source 10 to the scrambler 20 and also for controlling the new element, a seed source 16. The seed source 16 is coupled to the scrambler 20 through the same gate 15. In operation, prior to allowing data to be coupled to the scrambler 20, the timing and control 17 initiates transfer of a seed, from seed source 16 through the gate 15 to the scrambler 20. Once the seed has been transmitted to the scrambler 20, the timing and control 17

inhibits further operation of the seed source 16, and allows data to pass through the gate 15 to the scrambler 20. The manner in which these functions contribute to effect probabilistic scrambling is shown in more detail in Figure 4 which shows, in a schematic fashion, the elements of a suitable scrambler 20.

As shown in Figure 4, the input to the scrambler 20 from the gate 15 is coupled to one input of a XOR gate 25. The output of the XOR gate 25 is coupled to terminal 2 of a switch S_1. Another terminal, terminal 1, of the switch S_1 is coupled to a source of binary signals of a known pattern, e.g. all 0's. The common terminal of the single pole double throw switch S_1 is coupled to the input of a K-bit shift register 26. The K-bit shift register 26 is clocked by a clock source, not illustrated. Various stages of the shift register 26 are coupled to inputs of a second XOR gate 27. An output of the XOR gate 27 is coupled to one terminal of a single pole single throw switch S_2. The other terminal of the switch S_2 is coupled to the other input of the XOR gate 25. Finally, the output of the XOR gate 25 is also coupled to the modulator 30.

In operation, and prior to the transmission of a message, switch S_1 is set to position 1, and switch S_2 is open. This condition is maintained for a sufficiently long time to ensure that each stage of the K-bit shift register 26 has stored therein a "0".

In this condition, we can now select a K-bit seed. The K-bit seed (derived, for example, from the seed source 16) is input to the XOR gate 25, immediately preceding the data to be transmitted. In one embodiment of the invention, at the time the first bit of the seed is available at the XOR gate 25, the switch S_1 is switched to position 2, at the same time the switch S_2 is closed. This condition is maintained until the entire seed has been coupled through

the XOR gate 25. This seed is immediately followed by the data to be transmitted which is also coupled through the XOR gate 25. The path followed by the seed-data is from the gate 15, through the gate 25, through switch S_1 through the K-bit shift register, the gate 27, the switch S_2 (which is closed) and the XOR gate 25 to the modulator 30.

As each data bit (from gate 15) is presented to gate 25, it is XOR'ed with the output of gate 27 and the result (the transmitted signal) is passed on to modulator 30. The first K bits of the transmitted signal can be used to identify the seed, the following scrambled data can be used to derive the raw data.

Following the last data bit, the switches can be reset, the shift register cleared to zeros to accept the seed for the next message. Alternatively, the next message can follow immediately on the heels of the first and the position of the switches shown in Figure 4 are maintained; the seed source 16 remains inhibited, until such time as the timing and control 17 determines that a new seed should be employed. At that time, the process previously described is repeated.

The foregoing process results in a transmitted signal (the output of the gate 25 coupled to the modulator 30), forming two distinct portions (at least for the first message transmitted with a new seed). The first portion comprises the seed which has been scrambled (via the multiple connections to the gate 27 from different stages of the shift register) as well as the varying data inputs to the XOR gate 25. Following the transmission of the scrambled seed, the scrambled data is transmitted. Each subsequent message (transmitted without changing the seed) carries only scrambled data. This operation requires the shift register 26 to be in some known initial condition before the seed is introduced. During the data transmission period, gate 27

produces a scrambling bit sequence which is used to scramble the data.

It is also possible to transmit the seed in its unscrambled form, immediately followed by the scrambled data. This is an alternate method of operating the apparatus shown in Figure 4 and this alternate method is described as follows.

Just as in the operation above, every stage of the shift register 26 is set to 0. This is accomplished, for example, by maintaining switch S_1 in position 1, and clocking the shift register at least a number of times equal to its length, with switch S_2 maintained open. Once the K-bit shift register 26 has only 0's in each stage, switch S_1 is shifted to position 2 and switch S_2 is maintained open. After the seed has passed through the gates 15 and 25, it entirely fills the K-bit shift register. The seed, however, has also passed, unaltered to the mod 30 (via gate 25). The seed is unaltered since S_2 is open so the only input to gate 25 is the seed. Thereafter, switch S_2 is closed. The next data bit at the input to gate 25 from gate 15 is the first data bit. The switches (S_1 and S_2) are maintained in this condition as each bit of data is shifted through gate 25. After the scrambled data has been transmitted, the switches can be restored to their normal condition. Alternatively, the shift register can be maintained in its condition following the last data bit, and the next message can be immediately coupled through the gates 15, 25. With this alternate method of operation, the seed is transmitted (output to the modulator) in unscrambled form whereas the data which follows the seed has been scrambled.

The seed source 16 can provide a K-bit bit sequence which is random, each time the timing and control 17 indicates the necessity for a new seed. Alternatively, the seed source 16 may be merely a counter which is incremented each time a new

seed is employed. In this embodiment, each K-bit seed is in effect a count one higher than the preceding K-bit seed. In still further alternative, the seed produced by the seed source 16 can be a combination of the contents of a counter which is updated each time the seed source is addressed with the random bit sequence.

The shift register 26 shown in Figure 4 of course has multiple stages. Figure 4 is arranged to indicate that it does have multiple stages and has multiple connections to the gate 27; however, not all the stages are necessarily shown nor are all the connections to the gate 27 shown. Desirably, the K-bit shift register and the gate 27 are arranged as a linear feedback shift register to implement a polynomial which is primitive. The result of this apparatus (the output of the gate 27) is a maximum length sequence, suitably it should have high data transition density. For example, for a 15-stage shift register, the polynomial

$$g(x) = x^{15} + x^{12} + x^{8} + x^{4} + x^{2} + x + 1$$

is a good choice.

Figure 5 shows that in accordance with the method and apparatus of the invention, the descrambler 50 is associated with a timing and control 45. The descrambler 50 may take the form shown in Figure 6. Figure 6 illustrates a similar K-bit shift register 56, with an input provided through a switch S_3 (similar to the switch S_1 at the transmitter). Terminal 2 of switch S_3 is input from the demodulator 40, and is also coupled as one input to a gate 55. The K-bit shift register 56 is associated with a representative gate 54 (as is apparent to those skilled in the art, the gate 54 is representative of one or more of several other gates which are not illustrated, depending upon the particular polynomial chosen). The output of the gate 54 is coupled through a switch S_4 (similar to the switch S_2 at the

transmitter) to the other input of the gate 55. The output of gate 55 is coupled through an AND gate 57 to the data sink 60. The other input to the AND gate 57 is provided from the timing and control 45. As will be seen below, the output of the gate 55 includes K bits corresponding to the seed. Since this is not information which is required by the data sink 60, the timing and control 45, by controlling its input to gate 57 inhibits coupling this information to the sink 60. Accordingly, the timing and control 45 is arranged only to pass the (descrambled) data.

By manipulating switches S_3-S_4 in a manner similar to that of switches S_1-S_2, descrambling operation can be limited to descrambling only the data, or descrambling the seed as well. Of course, the selection of the mode of operation of switches S_3 and S_4 must be made depending upon the mode of operation taking place at the transmitter.

In general, the K-bit shift register 56 should exhibit a known bit pattern (identical to the known bit pattern used in register 26; in the example described here - all zeros) prior to a descrambling operation. This is effected in any well known manner, e.g. by maintaining the switch S_3 in position 1 for a sufficiently long period while the register is clocked. Thereafter, switch S_3 is moved to terminal 2, for inputting the seed and data. If the seed must be descrambled, the switch S_4 is closed at the same time switch S_3 is transferred to terminal 2. On the other hand, if the seed is not scrambled, then switch S_4 is maintained open until the entire seed has been stored in the shift register 56 and data begins arriving. Under these circumstances, of course, switch S_4 and gate 57 are enabled simultaneously.

Figures 7, 8 and 9 correspond to the different operational schemes at the transmitter (those skilled in the art will be

able to produce similar figures for descrambling operations).

More particularly, Figure 7 shows the states of the elements 10, 16, 20, S_1 and S_2, as a function of time. As shown in Figure 7, for example, switch S_1 is initially in position 1. It is maintained in this position sufficiently long to ensure that the contents of the K-bit shift register are cleared to 0. Thereafter, switch S_1 is switched to position 2, switch S_2 is closed and the K-bit seed is coupled from the seed source 16 through the gate 15. Following the last bit of the K-bit seed, the data source 10 couples the M-bit data sequence, also through the gate 15. The output of the scrambler 20 is also shown, as comprising a first portion which a scrambled K-bit seed, followed the scrambled M bits of data.

Figure 7 is arranged to illustrate this sequence repeats such that at the termination of the data, switch S_2 is open and switch S_1 is placed to its position 1 to again repeat the sequence.

Figure 8 is identical except that it illustrates that the length of the data sequence may actually be made up of plurality of different messages, even though only a single seed has been employed.

Figure 9 is different from either Figure 7 or 8. As shown in Figure 9, the sequence is identical except that S_2 is open until data begins arriving from the data source 10. As a result, the output of the scrambler is also in two portions, but in this case the K-bit seed is output in unscrambled form. This is followed by M bits of scrambled data.

It should therefore be apparent that the present invention provides for probabilistic scrambling. Firstly, each

message or a plurality of messages is associated with a different scrambling bit sequence. The scrambling bit sequence is that sequence coupled through the switch S_2 to the XOR gate 25 at the time the data from data source 10 is input to the XOR gate 25. Accordingly, for appropriate descrambling to take place, the receiver must have some knowledge of the scrambling bit sequence. This knowledge can be obtained as shown in Figures 7-9 by preceding the transmission of the scrambled message with the seed, either in scrambled or unscrambled form. Although it is quite natural to transmit the seed before the message, since the seed must be used to descramble a message, it should also be apparent that it is within the scope of the invention to store the seed, transmit the scrambled message to be followed by the seed (in scrambled or unscrambled form). Alternatively, the seed can be transmitted via a parallel channel.

Alternatively, the seed or scrambled seed need not be transmitted at all so long as some data is transmitted sufficient to recreate at the receiver, the seed for descrambling purposes. Consider for example that the seed source 16 comprises a plurality of Q different seeds which are addressed by a counter, once following each transmission at which time the counter is also incremented. The receiver includes (for example within the timing and control block 45) a similar stored array of descrambling bit seeds therefor, also addressed by a counter. The logic of Figure 4 is altered by coupling the state of the counter to the modulator 30. In this arrangement, the output of the gate 25 is blocked for the period of time during which the seed would otherwise have been transmitted (in scrambled or unscrambled form), instead the state of the counter is coupled to the modulator 30. When the state of the counter has been transmitted, the XOR gate 25 is again coupled to the modulator 30 to transmit the scrambled data. At the receiver, receipt of the state of the counter is used to

address a descrambling bit sequence or seed. The connection from the demodulator to the descrambler is logically controlled so that until the scrambled data reaches the terminal 2, the output of the demodulator is blocked. Prior to that time, the appropriate descrambling bit sequence selected by this transmitted state of the counter is input to the K-bit shift register.

PROBABILISTIC SCRAMBLER AND METHOD OF PROBABILISTIC SCRAMBLING

CLAIMS

1. A method of scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking, comprising the steps of:

   a. generating a scrambling bit sequence;

   b. combining said scrambling bit sequence with said data for transmission to generate a transmitted signal, wherein the improvement comprises:

   c. periodically generating different scrambling bit sequences.

2. The method of claim 1 wherein said step (a) comprises:

   i. generating a seed,

   ii. loading said seed into a shift register,

   iii. shifting said seed through said register to generate said scrambling bit sequence,

   wherein said step (c) includes periodically generating a new seed.

3. A method of scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking, comprising the steps of:

a. generating a scrambling bit sequence,

b. combining said scrambling bit sequence with said data for transmission to generate said transmitted signal,

wherein the improvement comprises:

c. including bits in said signal transmission identifying said scrambling bit sequence.

4. The method of claim 3 wherein said bits identifying said scrambling bit sequence comprise a seed for generating said scrambling bit sequence.

5. The method of claim 3 wherein said bits identifying said scrambling bit sequence comprise an incrementing count for selecting an appropriate scrambling bit sequence.

6. Apparatus for scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking comprising:

a. means for generating a scrambling bit sequence,

b. means for combining said scrambling bit sequence with data for transmission to generate a transmitted signal, wherein the improvement comprises:

c. means for controlling said means for generating a scrambling bit sequence for periodically generating different scrambling bit sequences.

7. The apparatus of claim 6 wherein said means for generating a scrambling bit sequence comprises:

i. means for generating a seed,

ii. means for loading said seed into a shift register,

iii. and means for shifting said seed through said shift register to generate said scrambling bit sequence, wherein said means for controlling said means for generating a scrambling bit sequence includes means for periodically generating a new seed.

8. Apparatus for scrambling data for transmission to produce a signal for transmission providing reasonably frequent transitions for receiver clocking comprising:

a. means for generating a scrambling bit sequence,

b. means for combining said scrambling bit sequence with data for transmission to generate a transmitted signal,

wherein in the improvement comprises:

c. means for including in said signal transmission one or more bits identifying said scrambling bit sequence.

9. The apparatus of claim 8 wherein said means for inserting one or more bits identifying said scrambling bit sequence comprises means for generating a seed useful in generating said scrambling bit sequence.

10. The apparatus of claim 8 wherein said means for adding one or more bits to said signal transmission identifying said scrambling bit sequence includes a counter for identifying a selected one of a plurality of scrambling bit sequences.

FIG. 1

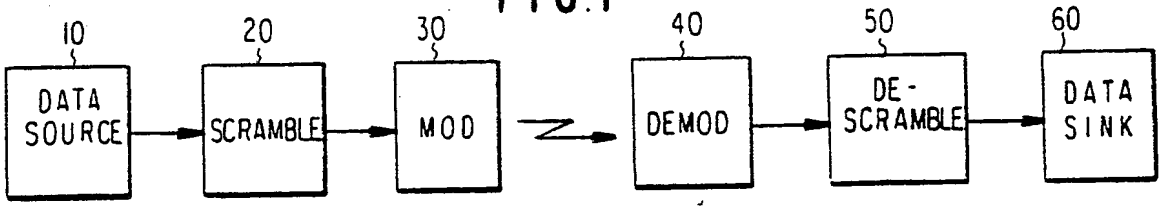


FIG. 2

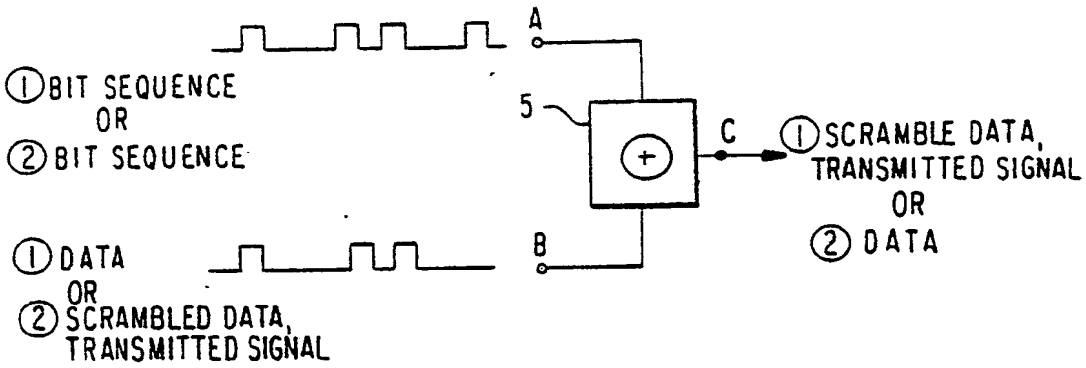


FIG. 3

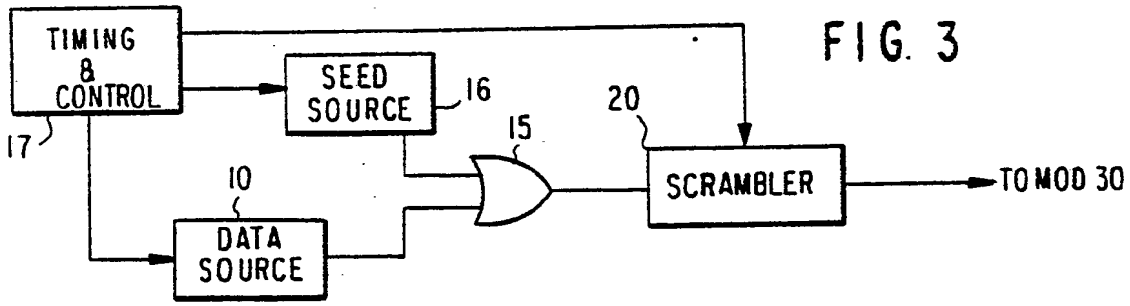


FIG. 4

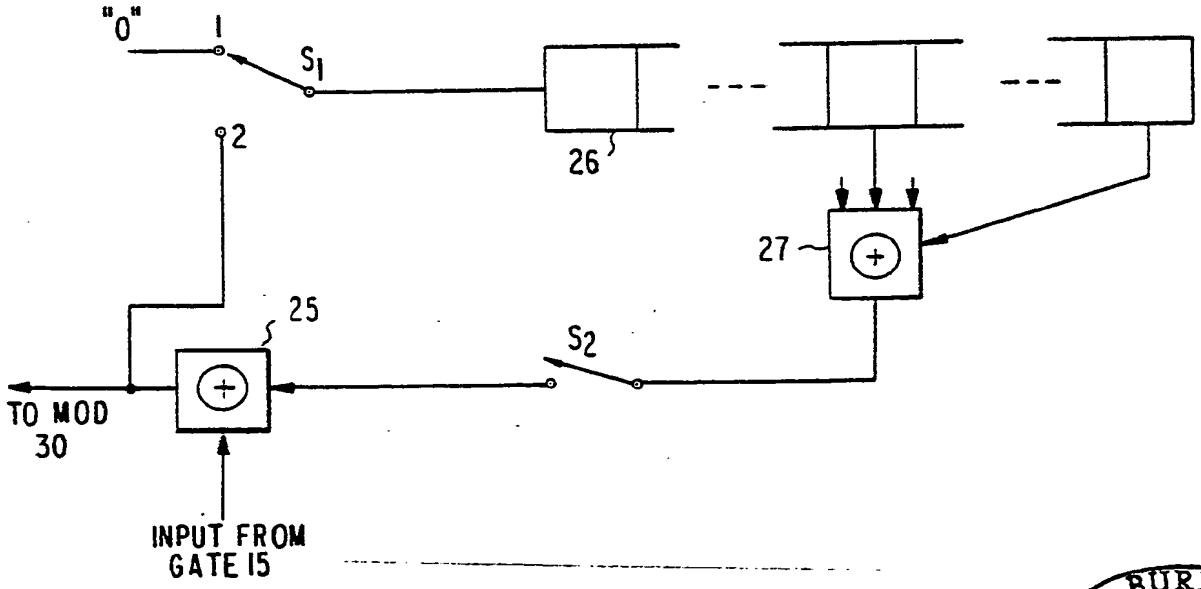


FIG. 5

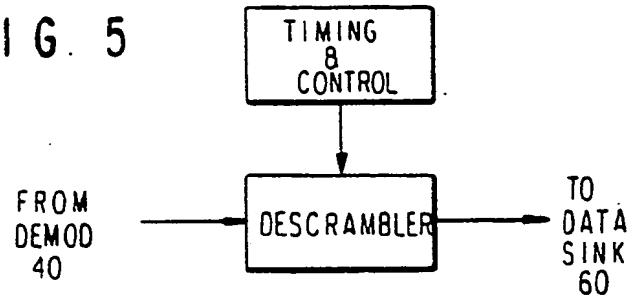


FIG. 6

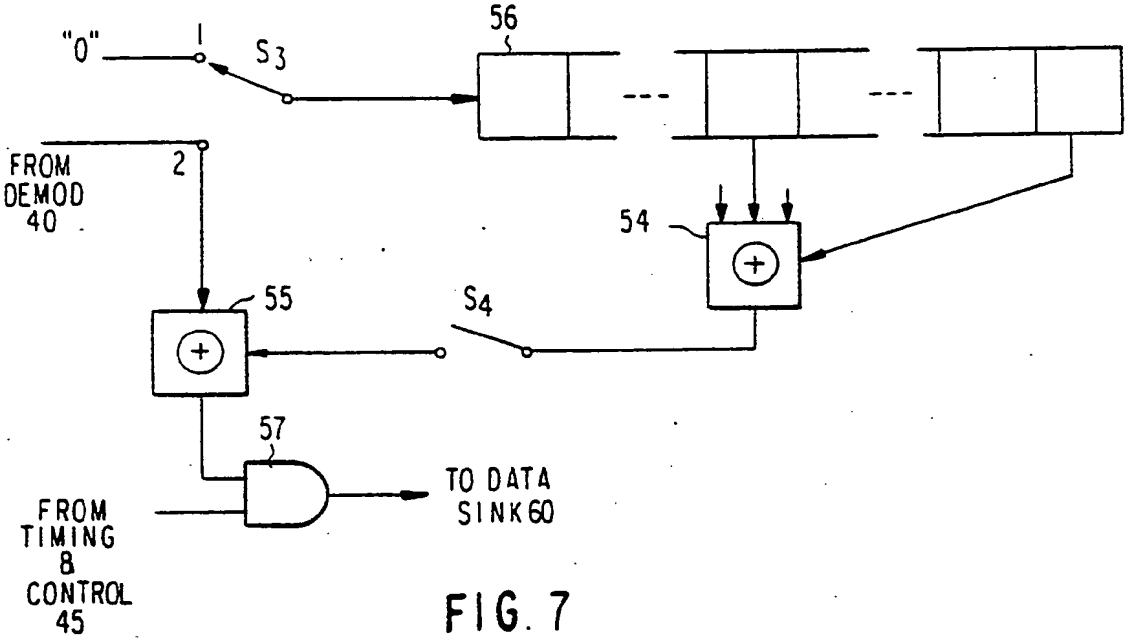


FIG. 7

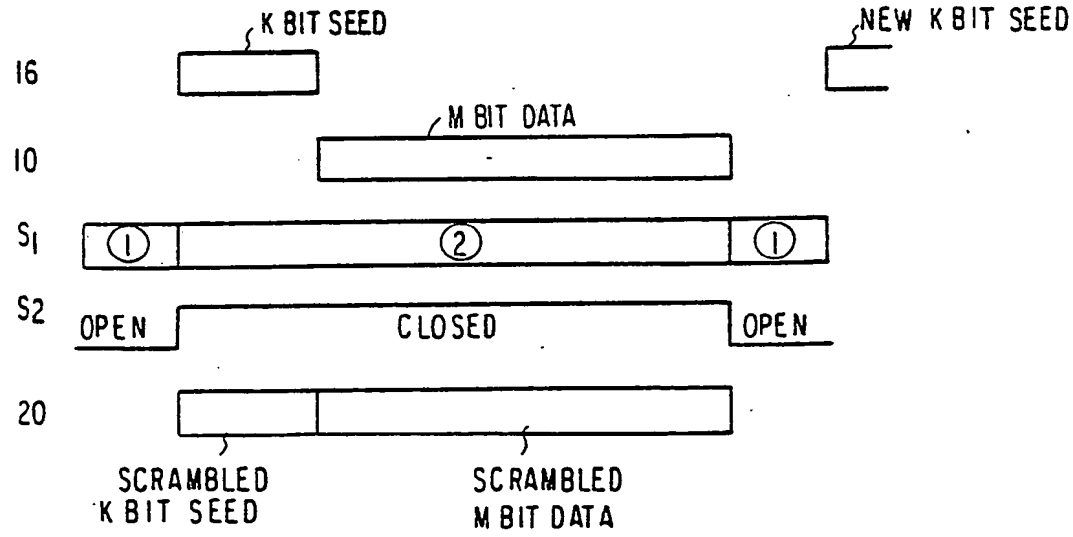


FIG. 8

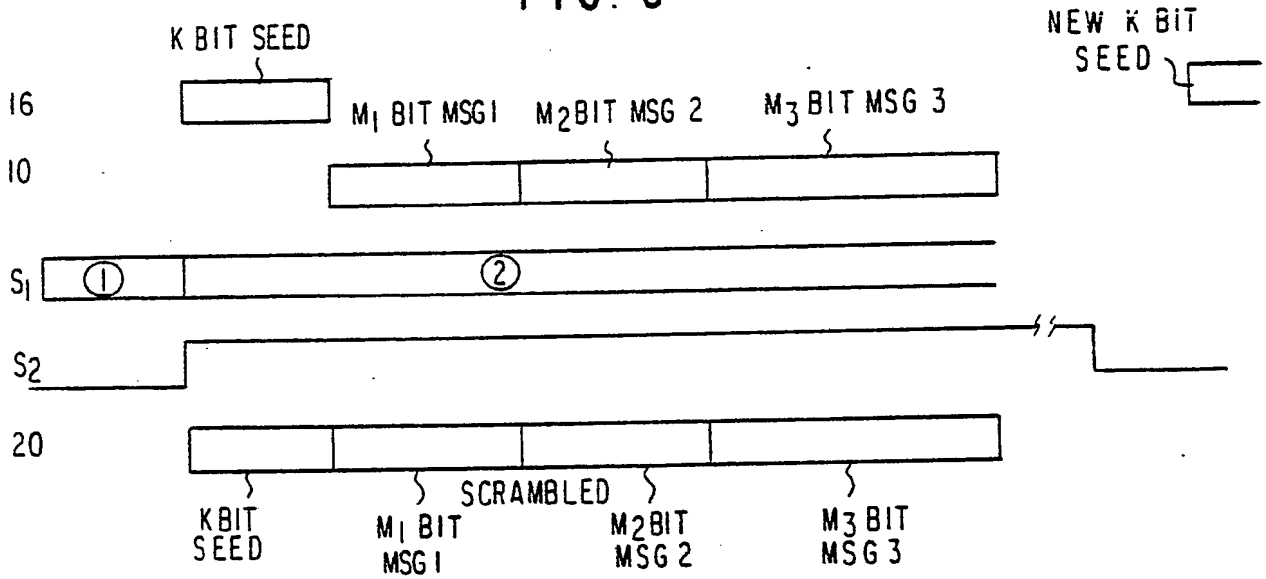
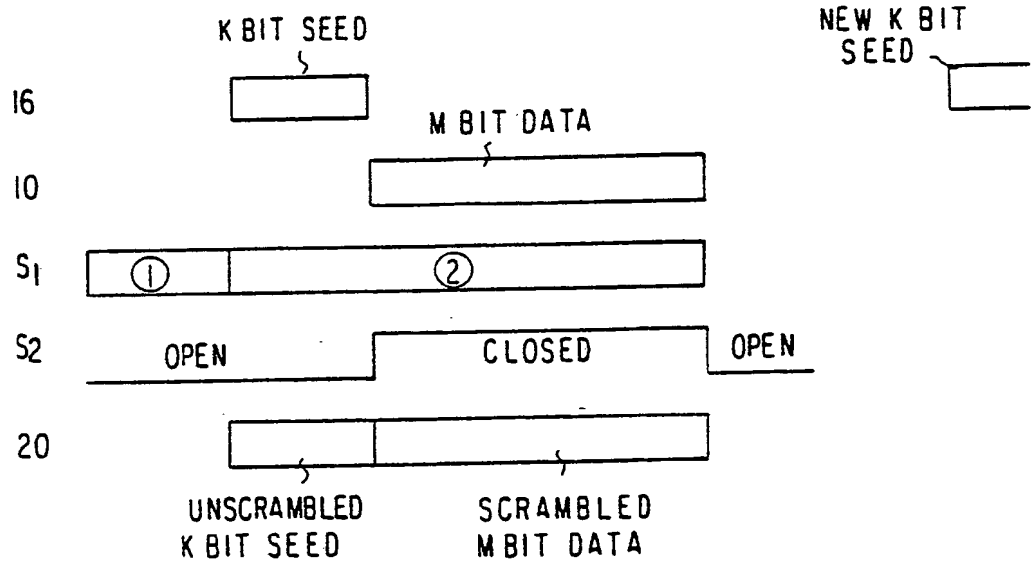


FIG. 9



INTERNATIONAL SEARCH REPORT

International Application No PCT/US84/01022

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) [3]

According to International Patent Classification (IPC) or to both National Classification and IPC

INT. Cl.[4] H04L 9/02, H04K 1/04, H04J 3/04

U.S. Cl. 375/1,2.1,2.2,115;178/22.04,22.17,22.19;179/1.5R,1.55;

II. FIELDS SEARCHED 370/80, 95, 104

Minimum Documentation Searched [4]

Classification System	Classification Symbols
U.S.	375/1,2.1,2,2,115; 178/22.04, 22.17, 22.19, 179/1.5R, 1.55; 370/180, 95, 104

Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched [5]

III. DOCUMENTS CONSIDERED TO BE RELEVANT [14]

Category *	Citation of Document, [16] with indication, where appropriate, of the relevant passages [17]	Relevant to Claim No. [18]
Y	US, A, 4,355,388 (Deal, Jr.) 19 October 1982, Col. 10, lines 30-40	1-11
Y	US, A, 4,264,781 (Oosterbaan et al) 28 April 1981 Col. 2	1-11
Y	US, A, 4,221,931 (Seiler) 9 September 1980	1-8
A	US, A, 4,214,209 (Baier et al)	1-8
Y	US, A, 3,808,536 (Reynolds)	1-8
Y	US, A, 4,052,565 (Baxter et al) 4 October 1974 Fig. 5	1-8
Y	US, A, 4,176,247 (England) 27 November 1979	1-8
Y	US, A, 3,522,374 (Abrahamsen et al) 28 July 1970	1-8

* Special categories of cited documents: [15]

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

IV. CERTIFICATION

Date of the Actual Completion of the International Search [2]	Date of Mailing of this International Search Report [2]
18 September 1984	21 SEP 1984
International Searching Authority [1]	**Signature of Authorized Officer [20]**
ISA/US	S.A. Cangialosi

Form PCT/ISA/210 (second sheet) (October 1981)